



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 150  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/698,498

10/30/2003

Sanjay Aiyagari

50325-0805

9591

29989

7590

05/02/2006

HICKMAN PALERMO TRUONG & BECKER, LLP

2055 GATEWAY PLACE

SUITE 550

SAN JOSE, CA 95110

EXAMINER

KIM, PAUL

ART UNIT

PAPER NUMBER

2161

DATE MAILED: 05/02/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

10/698,498

Applicant(s)

AIYAGARI ET AL.

Examiner

Paul Kim

Art Unit

2161

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 30 October 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-38 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-38 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 October 2003 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                        | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)               | Paper No(s)/Mail Date. _____  |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date <u>19 July 2004</u>  | 6) <input type="checkbox"/> Other: _____                                    |

Art Unit: 2161

### **DETAILED ACTION**

1. This Office Action is responsive to the following communication: Original Application filed on 30 October 2003.
2. Claims 1-38 are pending and present for examination. Claims 1, 10, and 18 are independent.

### ***Drawings***

3. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description:

- Figure 6A, reference character 612; and
- Figure 6B, reference character 312.

Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

### ***Specification***

4. The abstract of the disclosure is objected to because of undue length (i.e. exceeds 150 words). Correction is required. See MPEP § 608.01(b).

***Claim Rejections - 35 USC § 112***

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. **Claims 3, 6, 12, 15, and 20** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

7. **As per dependent claim 3**, the claim recites "an access identifier" in line 2 of the claim. It is unclear whether this is intended to be the same as or different from "access identifier" recited in lines 10 and 11 of claim 1.

Additionally, the claim recites "a group identifier file attribute" in lines 3-4 of the claim. It is unclear whether this is intended to be the same as or different from "a group identifier attribute" recited in line 7 of the claim.

8. **As per dependent claim 6**, the claim recites "a file operation" in line 3 of the claim. It is unclear whether this is intended to be the same as or different from "an operation on the file" recited in line 13 of claim 1.

9. **As per dependent claim 12**, the claim recites "a group identifier attribute" in line 3 of the claim. It is unclear whether this is intended to be the same as or different from "a group identifier attribute" recited in lines 10-11 of claim 10.

10. **As per dependent claim 15**, the claim recites "a file operation" in line 3 of the claim. It is unclear whether this is intended to be the same as or different from "an operation on the file" recited in line 13 of the claim 10.

11. **As per dependent claim 20**, the claim recites "a group identifier file attribute" in lines 3-4 of the claim. It is unclear whether this is intended to be the same as or different from "a group identifier attribute" recited in line 7 of the claim.

Art Unit: 2161

***Claim Rejections - 35 USC § 102***

12. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless --

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

13. **Claims 1-38** are rejected under 35 U.S.C. 102(b) as being anticipated by Barkley et al (U.S. Patent No. 6,202,066, hereinafter referred to as BARKLEY), filed on 18 November 1998, and issued on 13 March 2001.

14. **As per claims 1, 10, 18, 22, and 31**, BARKLEY teaches:

A method for controlling access to a resource, the method comprising the steps

of:

creating and storing in the Operating System filesystem a file that represents the resource {See BARKLEY, col. 2, lines 23-26, wherein this reads over "object security attributes are usually kept with the object (e.g., in the header of a file) and the object resides in (or a resource is accessed through) a single server"; and col. 4, lines 59-60, wherein this reads over "OATS can be created, edited, deleted, and assigned to or removed from objects. Each OAT thus defines an access control specification"};

receiving user-identifying information from a user requesting access to the resource {See BARKLEY, col. 1, lines 48-54, wherein this reads over "Windows NT allows various permission to be associated by the ACL with individuals or groups of individuals, so that the access sought is permitted"}, wherein the user-identifying information comprises a role associated with the user, wherein the role is determined from a user identifier uniquely associated with the user and from a group identifier associated with a group that includes the user {See BARKLEY, col. 2, lines 4-14, wherein this reads over "[u]ser security attributes may consist of defined groups ('roles') to which the user belongs, wherein access to various objects is permitted to all of the individuals identified as members of the group"};

receiving a resource identifier associated with the resource {See BARKLEY, col. 1, lines 22-27, wherein this reads over "'objects' may also include resources"; and col. 7, lines 22-26, wherein this reads over "a mechanism for mapping permissions authorized with respect to various objects to the corresponding identified individuals or groups"};

creating an access identifier based on the user-identifying information and the resource identifier, wherein the access identifier is formatted as a file attribute that is used by the Operating System to manage file access {See BARKLEY, col. 2, lines 23-26, wherein this reads over "object security attributes are usually kept with the object (e.g., in the header of a file) and the object resides in (or a resource is accessed through) a single server"; and col. 4, lines 59-60, wherein this reads over "OATS can be created, edited, deleted, and assigned to or removed from objects. Each OAT thus defines an access control specification"};

calling the Operating System to perform an operation on the file using the access identifier to gain access to the file {See BARKLEY, col. 8, lines 25-38, wherein

Art Unit: 2161

this reads over "In the Windows NT implementation mentioned . . . OATS [Object Access Type] which can be associated with objects, and writes the permissions and users (or roles) associated with each objects to the access control lists" and "access to a given object permitted only if an OAT assigned to that object itself indicated that the requestor was a member of a role having been assigned the permission sought with respect to the object"); and

granting the user access to the resource only if the Operating System call successfully performs the operation {See BARKLEY, col. 8, lines 25-38, wherein this reads over "access to a given object permitted only if an OAT assigned to that object itself indicated that the requestor was a member of a role having been assigned the permission sought with respect to the object"};

15. **As per dependent claims 2, 11, 19, 23, and 32, BARKLEY teaches:**

A method as recited in Claim 1, wherein the access identifier comprises:

a first set of bits for storing a role identifier, wherein the role identifier is associated with the role {See BARKLEY, col. 2, lines 4-14, wherein this reads over "user security attributes may consists of defined groups ('roles')"; lines 23-26, wherein this reads over "object security attributes are usually kept with the object (e.g., in the header of a file) and the object resides in (or a resource is accessed through) a single server"; and col. 4, line 47 – col. 5, line 4, wherein this reads over "Object Access Type" and "adding that role, assigned to those users, to the corresponding OAT"}; and

a second set of bits for storing the resource identifier {See BARKLEY, col. 4, lines 59-60, wherein this reads over "OATS can be created, edited, deleted, and assigned to or removed from objects. Each OAT thus defines an access control specification"}.

Furthermore, it would be inherent store both a role identifier and a resource identifier on a set of bits such that the set(s) of bits may be called and received by an Operating System as described in the aforementioned method of Claim 1.

16. **As per dependent claims 3, 20, and 24, BARKLEY teaches:**

A method as recited in Claim 1, wherein:

the step of creating an access identifier based on the user-identifying information and the resource identifier comprises formatting the access identifier as a group identifier file attribute {See BARKLEY, col. 7, lines 14-20, wherein this reads over "a simple mechanism for thus associating groups of object with sets of permissions and of users, organized as roles or groups"}; and

the step of calling the Operating System to perform an operation on the file representing the resource comprises:

assigning the access identifier to a group identifier attribute of an Operating System process {See BARKLEY, col. 9, lines 1-7, wherein this reads over "allowing a system administrator to add or remove a role or group from the OAT"}; and

calling an Operating System routine from the Operating System process to perform the operation on the file representing the resource {See BARKLEY, col. 8, lines 25-38, wherein this reads over "In the Windows NT

Art Unit: 2161

implementation mentioned . . . OATS [Object Access Type] which can be associated with objects, and writes the permissions and users (or roles) associated with each objects to the access control lists" and "access to a given object permitted only if an OAT assigned to that object itself indicated that the requestor was a member of a role having been assigned the permission sought with respect to the object").

**17. As per dependent claims 4, 13, 25, and 34, BARKLEY teaches:**

A method as recited in Claim 1,

wherein the step of calling the Operating System to perform an operation on the file representing the resource comprises comparing the access identifier to an identifier included in an Access Control List file attribute associated with the file representing the resource {See BARKLEY, col. 1, lines 48-54, wherein this reads over "access sought is permitted only if the user's identification matches the user entry in the ACL or the user is a member of a group entry in the ACL"};

wherein the Access Control List file attribute includes the identifiers of all users and all groups of users allowed to access the file representing the resource {See BARKLEY, col. 1, lines 48-54, wherein this reads over "a user entry in the ACL or the user is a member of a group entry in the ACL"};

**18. As per dependent claims 5, 14, 21, 26, and 35, BARKLEY teaches:**

A method as recited in Claim 1, wherein the operation on the file representing the resource is selected from a group consisting of opening the file, closing the file, deleting the file, reading from the file, writing to the file, executing the file, appending to the file, reading a file attribute, and writing a file attribute {See BARKLEY, col. 10, lines 56-61, wherein this reads over "possible Permissions are the usual NTFS file permissions: Read(R), Write(W), Execute(X), Delete(D), Change Permissions(P), and Take Ownership(O)"}.

**19. As per dependent claims 6, 15, 27, and 36, BARKLEY teaches:**

A method as recited in Claim 1, the method further comprising the steps of:

reading a permission bit associated with the file representing the resource, wherein the permission bit corresponds to a file operation performable on the file representing the resource {See BARKLEY, col. 1, lines 48-54, wherein this reads over "access sought is permitted only if the user's identification matches the user entry in the ACL or the user is a member of a group entry in the ACL"};

based on the file operation indicated by the permission bit, determining a resource operation that is performable on the resource {See BARKLEY, Figures 2, 4-5; and col. 9, lines 29-32, wherein this reads over "in green, if the selected role or group has all of the selected permissions"}; and

granting the user the privilege of performing the resource operation on the resource only if the permission bit allows the file operation to be performed on the file representing the resource {See BARKLEY, col. 8, lines 25-38, wherein this reads over "access to a given object permitted only if an OAT assigned to that object itself indicated that the requestor was a member of a role having been assigned the permission sought with respect to the object"}.

**20. As per dependent claims 7, 16, 28, and 37, BARKLEY teaches:**

Art Unit: 2161

A method as recited in Claim 1, the method further comprising the steps of:

opening the file representing the resource {See BARKLEY, col. 8, lines 31-38, wherein this reads over "access to a given object permitted only if an OAT assigned to that object itself indicated"};

reading from the file representing the resource a permission indicator associated with a resource operation {See BARKLEY, Fig 5; and col. 13, lines 28-49, wherein this reads over "allows a determination of permission provided by a role's membership in a hierarchy"}; and

enabling the user to perform the resource operation on the resource only if the permission indicator indicates that the user is allowed to perform the resource operation on the resource {See BARKLEY, Table 1; and col. 11, line 39 – col. 12, line 37, wherein this reads over "[v]arious roles have varied permission with respect to these files" and "only members of branch\_manager can delete these files"}.

21. **As per dependent claims 8, 17, 29, and 38, BARKLEY teaches:**

A method as recited in Claim 1, wherein the step of representing the resource by a file stored in the Operating System filesystem comprises:

creating the file representing the resource in the Operating System filesystem {See BARKLEY, col. 2, lines 23-26, wherein this reads over "object security attributes are usually kept with the object (e.g., in the header of a file) and the object resides in (or a resource is accessed through) a single server"; and col. 4, lines 59-60, wherein this reads over "OATS can be created, edited, deleted, and assigned to or removed from objects. Each OAT thus defines an access control specification"}; and

assigning an access value to a file attribute of the file representing the resource, the file attribute being used by the Operating System to manage file access, wherein the access value corresponds to a combination of a role and a resource {See BARKLEY, col. 10, lines 56-61, wherein this reads over "possible Permissions are the usual NTFS file permissions: Read(R), Write(W), Execute(X), Delete(D), Change Permissions(P), and Take Ownership(O)"}.

22. **As per dependent claims 9 and 30, BARKLEY teaches:**

A method as recited in Claim 8, wherein the file attribute used by the Operating System to manage file access is a group identifier file attribute {See BARKLEY, col. 9, lines 1-7, wherein this reads over "modify the permissions associated with that role or group, to assign objects to OAT designations or remove OATs from objects"}.

23. **As per dependent claims 12 and 33, BARKLEY teaches:**

A method as recited in Claim 10, wherein the step of making an Operating System call to perform an operation on the file representing the resource comprises:

storing the group identifier value of a group identifier attribute of an Operating System process {See BARKLEY, col. 2, lines 4-14, wherein this reads over "[u]ser security attributes may consist of defined groups ('roles') to which the user belongs, wherein access to various objects is permitted to all of the individuals identified as members of the group"};



Art Unit: 2161

assigning the access identifier to the group identifier attribute of the Operating System process (See BARKLEY, col. 2, lines 23-26, wherein this reads over "object security attributes are usually kept with the object (e.g., in the header of a file) and the object resides in (or a resource is accessed through) a single server"; and col. 4, lines 59-60, wherein this reads over "OATS can be created, edited, deleted, and assigned to or removed from objects. Each OAT thus defines an access control specification");

calling an Operating System routine from the Operating System process to perform the operation on the file representing the resource (See BARKLEY, col. 8, lines 25-38, wherein this reads over "In the Windows NT implementation mentioned . . . OATS [Object Access Type] which can be associated with objects, and writes the permissions and users (or roles) associated with each objects to the access control lists" and "access to a given object permitted only if an OAT assigned to that object itself indicated that the requestor was a member of a role having been assigned the permission sought with respect to the object"); wherein the operation on the file representing the resource is performed only if the value of the group identifier attribute of the Operating System process matches the value of the group identifier file attribute of the file representing the resource (See BARKLEY, Table 1; and col. 11, line 39 – col. 12, line 37, wherein this reads over "[v]arious roles have varied permission with respect to these files" and "only members of branch\_manager can delete these files"); and

resetting the group identifier attribute of the Operating System process to the stored group identifier value (See BARKLEY, col. 9, lines 1-7, wherein this reads over "allowing a system administrator to add or remove a role or group from the OAT").

### ***Conclusion***

24. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Deinhart et al (U.S. Patent No. 5,911,143) which discloses a method and system for registration, authorization, and control access rights in a computer system.
- Helland et al (U.S. Patent No. 6,014,666) which discloses a programming model for access privileges of roles.
- Anand et al (U.S. Patent No. 6,044,466) which discloses a mechanism that uses policy for combining the delegated permissions into the content's runtime permissions.
- Griffin et al (USPGPUB 2002/0178119) which discloses a method for managing access to resources with a role-based access control method.
- Kaiserwerth et al (USPGPUB 2003/0078932) which discloses a system wherein access permissions are provided by predefined user roles.

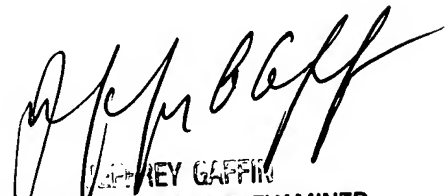
Art Unit: 2161

25. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul Kim whose telephone number is (571) 272-2737. The examiner can normally be reached on M-F, 9am - 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffrey Gaffin can be reached on (571) 272-4146. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Paul Kim  
Patent Examiner  
Art Unit 2161



JEFFREY GAFFIN  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100